Credential Spraying Risk Mitigation Plan

# Overview

The Credential Spraying Risk Mitigation Plan aims to minimize the threat posed by credential spraying attacks through a set of preventive measures, detection strategies, and response protocols.

# Objectives

* Reduce the likelihood of successful credential spraying attacks.
* Enhance the company’s ability to detect and respond to credential spraying attacks.
* Strengthen authentication mechanisms to withstand credential spraying attacks.
* Define requirements and increase employee awareness and training regarding credential hygiene and security best practices.

# Success metrics

* Reduction in successful credential spraying attacks by 90% within the first year.
* Increase in employee awareness and adherence to password hygiene practices.

# Roles

* Project manager: oversees team and progress of the project, updates stakeholders and upper management on current status, next steps, and any support needed.
* Security analysts: conduct risk assessments, draft password and account lockout policies, and design detection and response measures.
* IT administrators: work with security analysts to implement mitigation strategies.
* Training and education specialists: create credential hygiene and security awareness training.

# Scope and budget

* Focus on securing all externally facing authentication portals and services.
* Implementation of monitoring and detection mechanisms to identify suspicious authentication attempts.
* Education and training initiatives for employees regarding password hygiene and recognizing phishing attempts.

# Milestones

Phase 1: Risk Assessment and Planning

* Conduct a comprehensive risk assessment to identify vulnerable authentication points.
* Develop a detailed project plan outlining mitigation strategies, timelines, and responsibilities.
* Write strong password and account lockout policies.

Phase 2: Implementation of Preventive Measures

* Deploy multi-factor authentication (MFA) across all external-facing systems and services.
* Implement account lockout policies to prevent brute-force attacks.
* Enforce strong password policies including regular password rotations and complexity requirements.
* Implement IP-based blocking for suspicious login attempts.
* Integrate threat intelligence feeds to proactively identify potential credential spraying campaigns.

Phase 3: Enhancing Detection and Response Capabilities

* Implement real-time monitoring of authentication logs for anomalous activities.
* Configure alerts for suspicious login patterns indicative of credential spraying.
* Develop automated response mechanisms for immediate mitigation of detected attacks.
* Establish an incident response plan specifically tailored for credential spraying incidents.

Phase 4: Employee Training and Awareness

* Conduct regular security awareness training sessions focusing on password hygiene, phishing awareness, and recognizing suspicious activities.
* Provide guidance on creating strong, unique passwords and avoiding password reuse.
* Simulate credential spraying attacks to test employee response and effectiveness of security measures.

# Deliverables

* Completed risk assessment report.
* Completed password and account lockout policies.
* Configured monitoring and automated response mechanisms.
* Documentation of employee training sessions and awareness materials.

# Timeline

* Phase 1: Risk Assessment and Planning (2 months)
* Phase 2: Implementation of Preventive Measures (3 months)
* Phase 3: Enhancing Detection and Response Capabilities (2 months)
* Phase 4: Employee Training and Awareness (Ongoing, with initial sessions conducted within 1 month)